

UNITED STATES DISTRICT COURT

for the

\_\_\_\_\_ District of \_\_\_\_\_

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

)  
)  
)  
)  
)

Case No. MR 22-1698



APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

located in the \_\_\_\_\_ District of \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☐ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

The application is based on these facts:

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
\_\_\_\_\_  
(specify reliable electronic means).

Date: November 10, 2022

  
Judge's signature

City and state: \_\_\_\_\_

Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF A  
CELLULAR TELEPHONE, (1) BLUE  
MOTOROLA PHONE, IMEI  
359957730870076, CURRENTLY IN THE  
POSSESSION OF THE FEDERAL  
BUREAU OF INVESTIGATION OFFICE IN  
ALBUQUERQUE, NEW MEXICO

Case No. \_\_\_\_\_

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

I, Elia Viramontes, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in the possession of the Federal Bureau of Investigation, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since April of 2021. I have been a sworn law enforcement officer for approximately 7 years, serving as a police officer and special agent. I am currently assigned to the FBI Gang Task Force in Albuquerque, New Mexico (NM). Over the course of my career, I have arrested hundreds of individuals for crimes ranging from homicide, narcotics laws, robbery, assault and battery, and other violent crimes. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws. While employed by the FBI, I have gained experience through my training at the

FBI Academy, Quantico, Virginia. I have received training in a variety of investigations and legal matters, including drafting and executing search and arrest warrants.

**PURPOSE OF AFFIDAVIT**

3. I make this affidavit in support of an application for search warrant authorizing the search of the following property: (1) a Blue Motorola Phone, IMEI 359957730870076, hereinafter the “Device,” for evidence of violations of:

- a. Title 21, United States Code, Section 841(a)(1) - possession with intent to distribute a controlled substance;
- b. Title 21, United States Code, Section 843(b) - use of a communication facility in furtherance of drug trafficking;
- c. Title 18, United States Code, Section 922(g) - felon in possession of a firearm; and
- d. Title 18, United States Code, Section 924(c) – possession of firearm in furtherance of a drug trafficking crime.

4. The Device is currently maintained by the Federal Bureau of Investigation in Albuquerque, New Mexico. I seek authorization to search the Device for items described in Attachment B.

**PROBABLE CAUSE**

5. On November 2, 2022, the Honorable United States Magistrate Judge Jerry H. Ritter issued search warrants (22-MR-1612) authorizing the search of the residence of Elliott PERALTA a.k.a “CASH” (PERALTA), 537 Sky Tower Street SW, Albuquerque, New Mexico. The search authorized the search of the premises for evidence of conspiracies to distribute

controlled substances; unlawful firearms possession; and possession of a firearm in furtherance of a drug trafficking crime.

6. During the execution of the search warrant at 537 Sky Tower Street SW, Albuquerque, New Mexico, agents arrived at the residence, activated their emergency lights, knocked and announced at the front door. A dog was heard barking and after about 15 seconds a voice was heard inside. After approximately 30 seconds, cooperating witness (CW) opened the door and complied with officers. CW's identity is known to me however, I left identifying information out of the affidavit for their safety.

7. CW advised PERALTA and his girlfriend were still inside the residence. CW knew they were in the kitchen sometime before Agents arrived. Upon entrance to the residence Agents located the back sliding door partially open. No other persons were located inside the house until Agents were informed by CW that there was a secret room inside the master bedroom closet. Inside the secret room Agents located PERALTA's girlfriend Delilah FERNANDEZ who was hiding in the room with the door locked. FERNANDEZ stated her and PERALTA were in the kitchen prior to Agents' arrival. PERALTA went to the laundry room right before the first knock at the front door. FERNANDEZ and PERALTA had talked about hiding in the secret room if law enforcement arrived at the location. FERNANDEZ ran upstairs to the secret room thinking PERALTA was going to be behind her but when she got to the secret room, she realized they had gone separate ways. FERNANDEZ was detained and later taken into custody on a probation violation warrant regarding a 2020 FBI investigation wherein she was charged with felon in possession of a firearm and ammunition. When FERNANDEZ was escorted out of the residence,

she stated her purse was in the kitchen and her phone was in the living room. FERNANDEZ described her phone to be in a pink case.

8. Special Agent Jordan Spaeth interviewed FERNANDEZ after she was advised of her Miranda Rights, FERNANDEZ agreed to speak with SA Spaeth without her lawyer present. She advised she was a Burquena gang member and currently out on the run for a pending FBI felon in possession of a firearm case. She was dating PERALTA for just less than three years. FERNANDEZ stays at the residence off and on, and has clothes, court paperwork, and photographs of her and PERALTA in the residence. FERNANDEZ asked for an attorney when asked about her address. The interview was concluded, and no further questions were asked.

9. During the execution of the search warrant at 537 Sky Tower St SW, Agents located and seized the following property:

- a. Approximately one (1) kilogram of methamphetamine (found in the kitchen),
- b. Approximately 105 grams of blue "M30" pills containing fentanyl (found in the kitchen).
- c. Two cellphones: (1) blue Motorola with a pink case (found in the living room), (1) black nonfunctional iPhone 11 (found in the kitchen),
- d. One Springfield armory XD's Pistol serial number S3145041 (found in the kitchen),
- e. One Glock 43 pistol, serial number ZHP611 (found in the garage).

10. Agents located the phone with a pink case (the Device) in the living room area. Agent photographed the Device and noticed the Device was powered on, but the screen was locked and required a passcode to be unlocked. The Device screen lighted up and partial messages were observed from unsaved numbers requesting to meet up. The Device also had CashApp

transactions. In the kitchen there was a women's purse containing a bag with blue "M30" pills suspected to be fentanyl and drug paraphernalia.

### **EVIDENCE COMMONLY FOUND ON CELL PHONES AND COMPUTERS**

#### **Evidence of Narcotics Trafficking Frequently Found on Phones**

11. Based upon my training and experience, and that of other more experienced law enforcement officers, I know that drug dealers use cellular telephones as a tool or instrumentality in committing their criminal activity. They use them to maintain contact with their suppliers, distributors, and customers. They prefer cellular telephones because, first, they can be purchased without the location and personal information that land lines require. Second, they can be easily carried to permit the user maximum flexibility in meeting associates, avoiding police surveillance, and traveling to obtain or distribute drugs. Third, they can be passed between members of a drug conspiracy to allow substitution when one member leaves the area temporarily. Many of the drug dealers myself and other more experienced law enforcement officers have contacted have used one or more cellular telephones for his or her drug business. The cellular telephones are used to call, text, or otherwise communicate with suppliers and customers of illegal drugs. As a result, evidence of drug dealing can often be found in text messages, call logs, photographs, videos, and other stored data on the cellular phone.

12. I also know that it is common for drug traffickers to retain in their possession phones that they previously used, but have discontinued actively using, for their drug trafficking business. Based on my training and experience, and that of other more experienced law

enforcement officers, the data maintained in a cellular telephone used by a drug dealer is evidence of a crime or crimes. This includes the following:

- a. The assigned number to the cellular telephone (known as the mobile directory number or MDN), and the identifying telephone serial number (Electronic Serial Number, or ESN), (Mobile Identification Number, or MIN), (International Mobile Subscriber Identity, or IMSI), or (International Mobile Equipment Identity, or IMEI) are important evidence because they reveal the service provider, allow us to obtain subscriber information, and uniquely identify the telephone. This information can be used to obtain toll records, to identify contacts by this telephone with other cellular telephones used by co-conspirators, to identify other telephones used by the same subscriber or purchased as part of a package, and to confirm if the telephone was contacted by a cooperating source. System and configuration data can assist investigators in identifying the platform through which the device is operated, which can also serve as evidence of the user's access to various service platforms.
- b. The stored list, or call log, of recent received, missed, and sent calls is important evidence. It identifies telephones recently in contact with the telephone user. This is valuable information in a drug investigation because it will identify telephones used by other members of the organization, such as suppliers, distributors and customers, and it confirms the date and time of contacts. If the user is under surveillance, it identifies what number he called during or around the time of a drug transaction or surveilled meeting. Even if a contact involves a telephone user not part of the conspiracy, the information is helpful (and thus is evidence) because it

leads to friends and associates of the user who can identify the user, help locate the user, and provide information about the user. Identifying a defendant's law-abiding friends is often just as useful as identifying his drug-trafficking associates.

- c. Stored text messages, email messages, chats, multimedia messages, installed applications or other electronic communications are important evidence, similar to stored numbers. Agents can identify both drug associates, and friends of the user who likely have helpful information about the user, his location, and his activities. Additionally, these communications can serve as evidence of the user, associates, and friends engaging drug trafficking activity or otherwise discussing associated persons, plans, and encounters.
- d. Photographs, videos, and audio files on a cellular telephone are evidence because they help identify the user, either through his or her own picture, or through pictures, videos, or audio files of friends, family, and associates that can identify the user. Pictures, videos, and audio files may also identify associates likely to be members of the drug trafficking organization. Some drug dealers photograph or record groups of associates, sometimes posing with weapons and showing identifiable gang signs. Also, digital photos often have embedded "geocode" or GPS information embedded in them. Geocode information is typically the longitude and latitude where the photo was taken. Showing where the photo was taken can have evidentiary value. This location information is helpful because, for



example, it can show where coconspirators meet, where they travel, and where assets might be located.

- e. Any documents, spreadsheets, calendar, note, password, dictionary or database entries, as well as any business records, to include ledgers, receipts, invoices, shipping documents, inventories, customer lists, bank account information, accounting or business software, customer communications, email communications, website or Social Media sites used for the business, and other business records and information reasonably related to the operation of an illicit business related to the crimes above. These items may serve as evidence of drug trafficking activity by articulating plans, methods, or other information relevant to persons engaged in the illegal activity, and operations which serve as component pieces of the illegal activity.
- f. Internet or browser entries or history may serve as evidence of illegal activity by demonstrating knowledge or intent of the illegal activity, referencing individuals, things, or entities involved in the illegal activity, or documenting interest or research into relevant components or aspects of the illegal operation.
- g. Stored address records are important evidence because they show the user's close associates and family members, and they contain names and nicknames connected to phone numbers that can be used to identify suspects.
- h. Any content on the device contained within smartphone applications such as WhatsApp, Snapchat, Marco Polo, Facebook and others. Content within applications contained on the device can be evidence as they commonly reflect

communications between individuals and the user of the device and may provide information related to the illegal activity.

13. Based upon my training and experience, and that of other more experienced law enforcement officers, I know that unlicensed dealers of firearms may use cellular telephones as a tool or instrumentality in committing their criminal activity. They use them to maintain contact and facilitate transactions with their suppliers and customers. They prefer cellular telephones because, they can be easily carried to permit the user maximum flexibility in meeting associates and accessing information and other communications platforms, such as email or social media, which may also be used as an instrument of their criminal activity. The cellular telephones may be used to call, text, or otherwise communicate with suppliers and customers of firearms. As a result, evidence of unlicensed dealing of firearms can often be found in text messages, call logs, photographs, videos, and other stored data on the cellular phone.

14. As some unlicensed firearms dealers sell firearms to individuals without conducting a background check, some of their customers may, in fact, be prohibited from possessing firearms. Communications stored on cellular telephones, whether through text messages, email, social media conversations, or other mediums of communication, serve as evidence to confirm or disprove that the unlicensed dealer of firearms had reasonable cause to believe that individuals to whom they sold firearms were prohibited from possessing firearms.

15. Based on my training and experience, and that of other more experienced law enforcement officers, the data maintained in a cellular telephone used by an unlicensed dealer of firearms is evidence of a crime or crimes. This includes the following:

- a. The assigned number to the cellular telephone (known as the mobile directory number or MDN), and the identifying telephone serial number (Electronic Serial

Number, or ESN), (Mobile Identification Number, or MIN), (International Mobile Subscriber Identity, or IMSI), or (International Mobile Equipment Identity, or IMEI) are important evidence because they reveal the service provider, allow us to obtain subscriber information, and uniquely identify the telephone. This information can be used to obtain toll records, to identify contacts by this telephone with other cellular telephones used by suppliers or customers, and to identify other telephones used by the same subscriber or purchased as part of a package. System and configuration data can assist investigators in identifying the platform through which the device is operated, which can also serve as evidence of the user's access to various service platforms.

- b. The stored list, or call log, of recent received, missed, and sent calls is important evidence. It identifies telephones recently in contact with the telephone user. This is valuable information in an unlicensed dealing of firearms investigation because it will identify telephones used by other individuals such as suppliers and customers, and it confirms the date and time of contacts. If the user is under surveillance, it identifies what number he called during or around the time of a transaction or surveilled meeting. Even if a contact involves a telephone user not involved in the transaction, the information is helpful (and thus is evidence) because it leads to friends and associates of the user who can identify the user, help locate the user, and provide information about the user. Identifying a defendant's law-abiding friends is often just as useful as identifying their criminal associates.
- c. Stored text messages, email messages, chats, multimedia messages, installed applications or other electronic communications are important evidence, similar to

stored numbers. Agents can identify associates and friends of the user who likely have helpful information about the user, his location, and his activities. Additionally, these means of communication may serve as evidence of the user engaging in the business of dealing firearms without a license by arranging or discussing planned or past transactions, advertising firearms for sale, and seeking to identify and acquire firearms from suppliers.

- d. Photographs, videos, and audio files on a cellular telephone are evidence because they help identify the user, either through his or her own picture, or through pictures, videos, or audio files of friends, family, and associates that can identify the user. Some unlicensed dealers of firearms record or photograph firearms they have obtained and intend to sell. Also, digital photos often have embedded “geocode” or GPS information embedded in them. Geocode information is typically the longitude and latitude where the photo was taken. Showing where the photo was taken can have evidentiary value. This location information is helpful because, for example, it can show where involved individuals meet, where they travel, and where firearms might be located.
- e. Any documents, spreadsheets, calendar, note, password, dictionary or database entries, as well as any business records, to include ledgers, receipts, invoices, shipping documents, inventories, customer lists, bank account information, accounting or business software, customer communications, email communications, website or Social Media sites used for the business, and other business records and information reasonably related to the operation of an illicit business related to the crimes above. These items may serve as evidence of

engaging in the business of dealing in firearms without a license by articulating plans, methods, or other information relevant to persons engaged in the illegal activity, and operations which serve as component pieces of the illegal activity.

- f. Internet or browser entries or history may serve as evidence of illegal activity by demonstrating knowledge or intent of the illegal activity, referencing individuals, things, or entities involved in the illegal activity, or documenting interest or research into relevant components or aspects of the illegal operation.
- g. Stored address records are important evidence because they show the user's close associates and family members, and they contain names and nicknames connected to phone numbers that can be used to identify suspects.
- h. Any content on the device contained within smartphone applications such as WhatsApp, Snapchat, Marco Polo, Facebook and others. Content within applications contained on the device can be evidence as they commonly reflect communications between individuals and the user of the device and may provide information related to the illegal activity.

### **TECHNICAL TERMS**

16. Based on my training and experience, and that of other more experienced law enforcement officers, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call

log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

17. Based on my knowledge, training, and experience, and that of other more experienced law enforcement officers, I know that cellular telephones, can store information referenced above for long periods of time. This information can sometimes be recovered with forensic tools.

18. *Forensic evidence.* As further described in ATTACHMENT B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because cellular telephones retain call logs, texts, and photographs in the memory of the cellular telephone. Similar to a computer or other digital device this information is retained in phone until it is written over.

19. *Manner of execution.* Because this warrant seeks only permission to examine one cellular telephone already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises.

#### **DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES**

20. Based upon the evidence provided, it is reasonable to believe the Devices were utilized to further drug trafficking, and to and to facilitate the unlicensed dealing of firearms. Because of the manner in which the device was used it is reasonable to believe the Devices were used as an instrumentality of the crimes under investigation.

#### **SEARCH TECHNIQUES**

21. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit imaging or otherwise copying all data contained on the Device and will specifically authorize a review of the media or information consistent with the warrant. The Device will be disconnected from cellular and internet networks at the time of the search warrant's execution so as to ensure that only data contained on the Device will be imaged or otherwise copied.

22. In accordance with the information in this affidavit, law enforcement personnel will execute the search of the Device pursuant to this warrant as follows:

#### **Securing the Data**

23. In order to examine the Device in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of the Device.<sup>1</sup>

24. Law enforcement will only create an image of data physically present on or within the Device. Creating an image of the Device will not result in access to any data physically located elsewhere. However, Device that have previously connected to devices at other locations may contain data from those other locations.

### **Searching the Forensic Images**

25. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit.

---

<sup>1</sup> The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.




26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.


**CONCLUSION**

27. I submit that this affidavit supports probable cause to believe that the Device contains evidence of Title 21, United States Code, Section 841(a)(1) - possession with intent to distribute controlled substance; Title 21, United States Code, Section 843(b) - use of a communication facility in furtherance of drug trafficking; Title 18, United States Code, Section 922(g) - felon in possess firearm; Title 18, United States Code, Section 924(c) - possess firearm in furtherance of drug trafficking. As such, I hereby request a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

  
Elia Viramontes  
FBI Special Agent

Electronically submitted and telephonically sworn to me on November 10, 2022

  
Honorable Jerry H. Ritter  
United States Magistrate Judge  
District of New Mexico

**ATTACHMENT A**

The properties to be searched are the following cellular telephones:

1. A Blue Motorola, IMEI359957730870076 recovered from PERALRA's residence on November 4, 2022 belonging to Delilah FERNANDEZ. Currently in FBI custody. The warrant authorizes the seizure and forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

All records on the Device described in Attachment A that constitute evidence of Title 21, United States Code, Section 841(a)(1) - possession with intent to distribute controlled substance; Title 21, United States Code, Section 843(b) - use of a communication facility in furtherance of drug trafficking; Title 18, United States Code, Section 922(g) - felon in possession of a firearm; and Title 18, United States Code, Section 924(c) – possession of firearm in furtherance of a drug trafficking crime, to include:

- a. Information related to any firearm used during the course of the crimes listed above, including the identities of who owned, possessed, and used the firearms during the course of the crimes;
- b. Any communication with or among co-conspirators, suppliers, or customers related to the crimes listed above;
- c. Any information relating to the planned distribution or planned use of the proceeds of the crimes listed above;
- d. Any subscriber information or contact information to include, names, addresses, telephone numbers, email addresses or other identifiers;
- e. Any call log information, including missed, incoming and outgoing calls and any information associated with those numbers;
- f. Any photographs, video and audio files related to the crimes listed above;
- g. Any text messages, email messages, chats, multimedia messages, installed applications or other electronic communications related to the crimes listed above;
- h. Any documents, spreadsheets, calendar, note, password, dictionary or database entries related to the crimes listed above;
- i. Any business records, to include ledgers, receipts, invoices, shipping documents, inventories, customer lists, bank account information, accounting or business software, customer communications, email communications, website or Social

Media sites used for the business, and other business records and information reasonably related to the operation of an illicit business related to the crimes above.

- j. Any internet or browser entries or history;
  - k. Any system data or configuration information contained within the device
- 1) Any other user or system files and data, contained on the subject device itself or an attached peripheral device such as a sim card or micro SD card, which would constitute evidence of violations described above.
  - 2) Evidence of user attribution showing who used or owned the SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history; As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) any photographic or video format, and any content on the device contained within smartphone applications such as WhatsApp, Snapchat, Marco Polo, Facebook and others that are stored on the device.